УДК 343.98 **doi: 10.21564/2225-6555.2021.2.242807**

ІНТЕГРАЦІЯ ІННОВАЦІЙНИХ ТЕХНОЛОГІЙ У ДІЯЛЬНІСТЬ З РОЗСЛІДУВАННЯ ЗЛОЧИНІВ – ПРОВІДНИЙ НАПРЯМ ПІДВИЩЕННЯ ЇЇ ЕФЕКТИВНОСТІ

Павлюк Наталія Вікторівна,
канд. юрид. наук, доцентка кафедри криміналістики,
Національний юридичний університет
імені Ярослава Мудрого,
Україна, м. Харків
e-mail: nat.pavluk.np@gmail.com
ORCID 0000-0001-8058-3071

Стаття присвячена одному із сучасних і пріоритетних напрямів науково-технічного забезпечення слідчої діяльності. Наголошено, що боротьба з кіберзлочинністю є одним із найважливіших питань сьогодення. Зроблено висновок, що в умовах поширення в сучасному світі кіберзлочинності одним із пріоритетних напрямів науково-технічного забезпечення слідчої діяльності є впровадження новітніх засобів, методів і технологій електронного інтелекту для роботи з електронними доказами та захисту джерел електронної (цифрової) інформації.

Ключові слова: електронний інтелект; інформаційно-комунікаційні технології; науково-технічне забезпечення; слідча діяльність; цифрова криміналістика.

Постановка проблеми. У сучасному суспільстві кожний аспект життя людини тією чи іншою мірою пов’язаний із використанням інформаційно-комунікаційних технологій, різних технічних і технологічних засобів. Мобільні телефони, смартфони, комп’ютери, ноутбуки чи планшетні ПК стали невід’ємною частиною повсякденного життя й посідають у ньому важливе місце. Доступ до Інтернету, онлайн-транзакції чи відправка SMS, MMS тощо потребують лише одного «кліку». Величезні обсяги даних, у тому числі й особистих, зберігаються у кіберпросторі. Однак епоха науково-технічної революції забезпечила передовими технологіями та інструментами й злочинний світ, який використовує їх для отримання різного роду конфіденційних даних й обертає їх на власну користь. Таким чином, сьогодні під загрозою кіберзлочинності знаходяться бізнес, промисловість, державні установи та інфраструктура, а також персональна безпека окремих громадян.

Аналіз останніх досліджень і публікацій. Окремі аспекти проблеми, пов'язаної з науково-технічним забезпеченням слідчої діяльності, висвітлено у працях Г. К. Авдєєвої (G. K. Avdeeva), П. В. Берназа (P. V. Bernaz), В. В. Білоуса (V. V. Bilous), В. А. Журавля (V. A. Zhuravel), М. В. Кобця, (M. V. Kobets), С. С. Паламарчука (S. S. Palamarchuk), Л. Д. Удалової (L. D. Udalova), В. Ю. Шепітька (V. Yu. Shepitko) та ін. [1–5]. Втім рівень поширення злочинів у сфері телекомунікацій та інформаційних технологій і комп'ютерних систем, а також удосконалення способів їх вчинення потребує значної уваги та подальшого наукового розроблення питань щодо вдосконалення, створення та впровадження апаратних і програмних інструментів, прийомів і методів їх застосування для захисту джерел електронної (цифрової) інформації, а також збирання та дослідження доказів у віртуальному просторі з метою протидії кіберзлочинності.

Метою статті є висвітлення питань, пов'язаних з одним із сучасних напрямів науково-технічного забезпечення слідчої діяльності – технологіями електронного інтелекту.

Досягнення поставленої мети зумовило необхідність вирішення таких **завдань**: а) дослідити специфіку інноваційних продуктів для роботи з електронною (цифровою) інформацією та захисту її джерел; б) розкрити сутність одного з провідних напрямів науково-технічного забезпечення слідчої діяльності.

Виклад основного матеріалу. На сьогоднішній день поняття «кібертероризм», «кіберзлочинність», «комп'ютерна злочинність» включає всі протизаконні дії, при яких електронне опрацювання інформації було знаряддям їх вчинення або об'єктом. Таким чином у це коло проблем потрапили не лише злочини, безпосередньо пов'язані з комп'ютерами, електронно-комунікаційними системами й мережами, але й такі, як шахрайство з кредитними магнітними картками, злочини у галузі телекомунікацій (шахрайство з оплатою міжнародних телефонних переговорів), незаконне використання банківської мережі електронних платежів, програмне

«піратство», шахрайство з використанням ігрових автоматів та багато інших злочинів. До цієї групи також відносяться питання, пов'язані з електронними доказами комп'ютерного походження, які використовуються при запобіганні та розслідуванні традиційних злочинів [6].

Наразі в Україні у повному обсязі присутні всі ключові «класичні» кіберзлочини, що вчиняються за допомогою комп'ютерних і телекомунікаційних технологій, кількість яких щороку зростає. Це розповсюдження комп'ютерних вірусів, шахрайства з платіжними картками, крадіжки грошей з банківських рахунків, викрадення інформації, онлайн-торгівля наркотиками та зброєю, формування у дітей суїцидальної поведінки тощо [7]. Так, у 2018 р. працівниками Департаменту кіберполіції виявлено близько 6 тис. злочинів, вчинених у сфері використання високих інформаційних технологій. З них майже тисяча – злочини, вчинені у сфері кібербезпеки. Затримано організатора бот-мережі Аваланч, викрито учасника міжнародного хакерського угрупування Кобальт, взято участь у припиненні діяльності міжнародної хакерської групи FIN7 (ФинСевен). Також за рік попереджено поширення чотирьох масових кібератак на території України. Затримано кілька організованих злочинних груп, які спеціалізувалися на створенні фіктивних бірж з продажу цінних паперів. Протягом року припинено діяльність понад 40 піратських сайтів. У межах міжнародної співпраці викрито 8 транснаціональних хакерських угруповань та взято участь у понад 30 міжнародних операціях [8]. За результатами роботи співробітників Національної поліції України у 2019 р. викрито 4 263 кіберзлочини [7]. Відповідно до статистичної інформації про кримінальні правопорушення та результати їх досудового розслідування тільки у січні-лютому 2020 р. було зареєстровано 438 кіберзлочинів і ці відомості стосуються лише тих, що передбачені Розділом XVI КК України. Причому переважна їх більшість пов'язана з несанкціонованим втручанням в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку та несанкціонованих дій з інформацією, яка

оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (статті 361, 362 КК України) [9]. Загалом минулого року було зареєстровано понад 5 тис. кіберзлочинів, за які оперативно затримали 106 фігурантів кримінальних проваджень, серед них 13 педофілів [10].

Проте говорити сьогодні про дані, які повно й достовірно відображали б стан і структуру кіберзлочинності в Україні, проблематично, оскільки дотепер у національному і навіть міжнародному законодавстві бракує єдиного підходу до визначення підстав віднесення протиправних діянь до категорії кіберзлочинів. Якщо у звіті Національної поліції України містяться дані про певну кількість злочинів, які можна віднести до кіберзлочинів, в офіційних статистичних звітах, крім Розділу XVI КК України, такі показники відсутні. Крім того, варто відмітити й високий рівень латентності кіберзлочинності (наразі обліковується тільки 10–20 % вчинених злочинів, а решту становить латентна злочинність) [11].

В останні роки кіберзлочинність стала більш організованою і набула ознак бізнесу, в якому важливими складовими є прибуток та опанування нових ринків. Відбувається зрощення національних злочинних угруповань з транснаціональними злочинними організаціями. Зростає не тільки організованість кримінальних груп, але й їх законспірованість, збільшується кількість осіб, що займаються протиправною діяльністю в Інтернеті на професійній основі, посилюється спеціалізація таких осіб. Як приклад функціонування транснаціональної злочинної групи можна навести протиправну діяльність з торгівлі персональними даними в мережі «Даркнет», організованої громадянином України. У 2018 р. працівники Департаменту кіберполіції Національної поліції України встановили чотирьох українців, які причетні до створення, організації та адміністрування однієї із найвідоміших у мережі «Даркнет» онлайн-платформи з продажу персональних даних користувачів мережі. До документування цієї злочинної групи були залучені правоохоронці Домініканської Республіки, Індонезії, Іспанії, Франції та

України. Хакери впродовж останніх п'яти років безперешкодно отримували доступ до облікових записів «PayPal», «Amazon», «eBay», «WellsFargo», «Suntrust», «Bank of America». Постраждалими від їхніх дій стали як громадяни України, так і мешканці Канади, Великобританії, Іспанії, Франції [12].

Навіть зараз, у період глобальної пандемії COVID-19, хакери швидко скористалися ситуацією та активізували свої атаки із застосуванням шкідливого програмного забезпечення і використовуючи панічні настрої серед громадян, здійснюють фішинг-атаки. Хакери замаскували свої атаки під інформування громадян про розвиток пандемії. Найчастіше, аби ввести в оману, вони використовують у своїх фішинг-розсилках посиланням на слово «Corona», а також розповсюджують шкідливе програмне забезпечення шляхом копіювання інформаційних панелей організацій, що надають актуальну інформацію про COVID-19 [13].

Будь-яке розслідування злочинів або судовий розгляд – «боротьба за інформацію». Недостатність інформації (відсутність доказів або їх хибність) ускладнює процес встановлення факту вчиненого злочину, винуватих осіб, мотивів злочину тощо. Інформатизація соціального середовища призвела до «технологізації» криміналістики. Фактично можна констатувати появу окремого криміналістичного напряму – «цифрової криміналістики» [14, с. 148].

Отже, невід'ємним і необхідним інструментом у боротьбі з кіберзлочинністю є цифрова криміналістика, яка застосовується для ідентифікації, збереження, відновлення, аналізу та презентації електронних доказів, знайдених у комп'ютерах чи цифрових пристроях зберігання даних. Термін «цифрова криміналістика» раніше використовувався як синонім комп'ютерної криміналістики, який українська мова запозичила з англійської (forensics – від англ. forensic science) – напрям криміналістики, що вивчає комп'ютерні злочини й має назву «computer forensics», але при запозиченні термін дещо звузив своє значення. Тому в нашій країні форензіка означає суто комп'ютерну криміналістику, а термін «цифрова криміналістика» має більш широке значення [15].

В Україні цифрова криміналістика є відносно новим науковим напрямом, де практичний досвід і технології у протидії злочинам, що вчиняються з використанням цифрових технологій, та у боротьбі з кіберзлочинністю лише починають накопичуватися. Серед актуальних й водночас малодосліджених питань залишаються проблеми, пов'язані з пошуком, фіксацією та дослідженням електронної (цифрової) інформації під час досудового розслідування й подальшого її використання як доказів у кримінальному провадженні. Усе це зумовлює необхідність застосування новітніх науково-технічних засобів, сучасних криміналістичних методів, спеціальних знань під час виявлення та фіксації слідів злочину в цифровій формі, специфічного порядку перевірки та оцінки таких доказів, а також спрямованих на посилення їх захисту від дистанційного знищення чи зміни [16, с. 53].

Виокремлюють такі галузі цифрової криміналістики:

1) комп'ютерна (форензіка) – основна мета якої полягає в інтерпретуванні поточного стану комп'ютерної системи, носіїв інформації та електронних документів. Комп'ютерна криміналістика охоплює широке коло інформації: від журналів (наприклад, історії з Інтернету) до фактичних файлів на диску;

2) криміналістика мобільних пристроїв – від комп'ютерної вона відрізняється тим, що мобільні пристрої мають вбудовану систему зв'язку. Дослідження орієнтовані на дані дзвінків та повідомлень (SMS, Email) і на глибоке відновлення видалених даних. Мобільні пристрої також корисні для надання інформації про місцезнаходження. Її можна відстежити через журнал дзвінків або за допомогою GPS;

3) мережева криміналістика – займається аналізом і відстеженням мережевого трафіку, локального і глобального Інтернету, збором доказів і виявленням вторгнень у систему [17];

4) медіа (відео, аудіо, зображення) – вилучення даних з DVR, покращення якості відео та зображень, виявлення слідів монтажу і редагування, автоматизована обробка з виділенням подій і об'єктів [18].

На сьогоднішній день існує безліч науково-технічних засобів для

вирішення завдань цифрової криміналістики, які класифіковані за різними категоріями: для збору даних; перегляду та аналізу файлів; аналізу реєстру; інтернет-аналізу; аналізу електронної пошти та мобільних пристроїв; аналізу Mac OS; мережевої криміналістики; експертизи бази даних тощо [19]. Прикладом програмного забезпечення для персонального комп'ютера є продукт Legal Tech, який протягом багатьох років використовується для вилучення доказів у ході кримінальних розслідувань, надає можливість автоматично отримувати текстові дані резервного копіювання розмов LINE зі смартфона Android і відображення повідомлення в хронологічному порядку. Елементами вилучення даних є: інформація про смартфон: назва виробника, назву моделі, номер IMEI, версія Android, дата і час опитування, зведення результатів опитування; запис інформації: історія дзвінків, телефонна книга, пошта оператора, SMS, LINE, текст LINE, WeChat, WhatsApp, FB Messenger, Twitter, історія, пов'язана з Інтернетом (історія відвідувань сайту, закладки, історія пошуку); зображення і відео: JPEG, GIF, PNG, MP4. Вихідний формат: Excel.xlsx, (дані вилучення скриншота відображаються в HTML і підтримується друк звітів). Екран вилучення: автоматичний скріншот; показ результату вилучення в HTML; пошук персонажів у розмовах. Резервне копіювання LINE. Автоматичне отримання: автоматичне отримання текстових даних резервного копіювання розмов LINE і відображення повідомлення в хронологічному порядку [20].

AOS Image Analysis Forensics Professional – це інструмент для аналізу відео, який виявляє фрагментовані відеокадри і витягує їх як докази. Навіть якщо заголовок відеофайлу перезаписаний, пошкоджений або не підтримує

ОС, відеоданні відновлюються і використовуються як докази. Відеодані можна відновити, навіть якщо файл видалений або пошкоджений, носій відформатований або програвач пошкоджений. Витягування відеоданих з різних файлових систем, пристроїв й кодеків. AOS Image Analysis Forensics Professional має не тільки функції вилучення та відновлення доказів, але також й функції покадрового зберігання нерухомих зображень і відтворення відео,

необхідні для судової експертизи [21].

Одним із прикладів технічних засобів цифрової криміналістики може слугувати апаратне забезпечення цілісності даних – дубликатор DemiUAv3. Ультракомпактний, легкий (близько 1 кг), високопродуктивний він ідеально підходить для перенесення та роботи на місці проведення слідчих (розшукових) дій. Цей продукт розроблений для збору, копіювання, аналізу цифрових доказів. Незважаючи на невеликий розмір, швидкість передачі даних становить близько 15 сек. на ГБ. Оснащений діагностичною функцією [22]. Слід сказати, що це одні з небагатьох інструментів, які використовуються співробітниками правозастосовних органів, спеціалістами та експертами для роботи з електронними (цифровими) слідами.

Серед актуальних питань криміналістики залишаються ті, що пов'язані з розробленням та використанням інноваційних технологій для захисту джерел електронної (цифрової) інформації й запобігання злочинам у сфері телекомунікацій та інформаційних технологій і комп'ютерних систем з метою протидії кіберзлочинності.

Одним із прикладів передових технологій для захисту кіберпростору від зловмисників є TrapX DeceptionGrid – потужна обман технологія, за допомогою якої вирішуються такі важливі питання, як: швидке виявлення кібератаки у реальному часі; з'ясування намірів атакувальників, їх тактики та інструментів; зупинення дій злочинців у всіх областях мережі й на кожному етапі атаки; забезпечення повернення до нормальних операцій. Даний продукт може імітувати дії справжніх користувачів, що створює у зловмисників помилкове відчуття успішної атаки – коли насправді вони взаємодіють тільки зі штучним користувачем всередині складної кібер-пастки, яка викриває хакерів і їх новітню тактику, зберігаючи при цьому мережу повністю захищеною [23]. Обман здійснюється з використанням приманки (підроблених даних і конфігурації на реальних кінцевих точках, які заманюють зловмисників у пастки) і пасток (це підроблені поверхні атаки, які були замасковані під мережеві активи) [24]. Нові покоління кібер-пасток можуть ідеально імітувати

операційні технологічні пристрої, такі як промислові компанії Rockwell і Siemens контролери. Зловмисники не можуть визначити, чи знаходяться вони у пастці або в реальній системі. Пастки, що імітують банкомати, торгові термінали, компоненти фінансової мережі SWIFT™ та багато іншого, можуть бути швидко розгорнуті [23]. Виявлення порушень і аналіз шкідливих програм сповіщають про події й візуалізуються за допомогою графіка часу атаки. Починаючи з моменту виявлення, DeceptionGrid автоматично збирає інформацію, потім розгортає і маскує пастки. Даний продукт надає криміналістичну інформацію, яка автоматично відправляється для обробки та аналізу. Як тільки аналіз завершено, результати відправляються назад і відбиваються у звіті. Візуалізація показує елементи атаки, такі як з'єднання, що дозволяє командам SOC або аналітикам краще зрозуміти, що в цей час відбувається у системі [24].

Висновки. Слідча та судова практика свідчить, що на даному етапі цивілізаційного розвитку світу виникають все нові й нові загрози, виклики й небезпеки у сфері критичної інформаційної інфраструктури держав, а також електронної інфраструктури відомств, установ та організацій. Це обумовлено тим, що постійно з'являються нові види міждержавних (транскордонних, транснаціональних, трансконтинентальних, планетарних) кіберзлочинів, які раніше взагалі не зустрічалися в слідчо-судовій практиці. Зокрема, це кіберзлочини, які вже сьогодні вчиняються в світовому космічному просторі, а також кіберзлочини, які вчиняються з використанням новітніх засобів, методів і технологій електронного інтелекту [6].

Отже, можна стверджувати, що одним із пріоритетних напрямів науково-технічного забезпечення слідчої діяльності в сучасних умовах є впровадження новітніх засобів, методів і технологій електронного інтелекту. Йдеться про вдосконалення та створення апаратних і програмних інструментів, прийомів і методів їх застосування для захисту джерел електронної (цифрової) інформації, а також збирання та дослідження доказів у сфері телекомунікацій та інформаційних технологій і комп'ютерних систем з метою протидії кіберзлочинності.

Список літератури

1. Інновації в криміналістиці. Інноваційні засади техніко-криміналістичного забезпечення діяльності органів кримінальної юстиції : монографія / кол. авт. : В. Ю. Шепітько, В. А. Журавель, Г. К. Авдєєва та ін. ; за заг. ред. В. Ю. Шепітька, В. А. Журавля. Харків : Апостіль, 2017. 260 с.

2. Берназ П. В. Інновації – основа криміналістичного забезпечення діяльності з розслідування злочинів. *Південноукраїнський правничий часопис*. № 4. 2015. С. 49–53.

3. Кобець М. В. Науково-технічне забезпечення розкриття та розслідування злочинів, пов'язаних з вибухами : автореф. дис. … канд. юрид. наук. Київ : Київ. нац. ун-т внутр. справ, 2006. 20 с.

4. Паламарчук С. С. Науково-технічне забезпечення пошуку слідів злочину у водному середовищі. *Науковий вісник Нац. акад. внутр. справ України*. Київ, 2004. № 2. С. 110–122.

5. Удалова Л. Д. Науково-технічне забезпечення отримання вербальної інформації. *Засади кримінального судочинства та їх реалізація в законотворчій і правозастосовній діяльності* : тези доп. та повідомл. наук.-практ. конф. (Київ, 3 квіт. 2009 р.). Київ : Атіка, 2009. С. 435–440.

6. Біленчук П., Малій М. Космічна й електронна кіберзлочинність: загрози і виклики нового тисячоліття. *Lexinform*. *Юридичні новини України.* URL: https://lexinform.com.ua/dumka-eksperta/kosmichna-j-elektronna-kiberzlochynnist-zagrozy-i-vyklyky-novogo-tysyacholittya/ (дата звернення: 26.09.2021).

7. Звіт Голови Національної поліції України про результати роботи відомства у 2019 році / Урядовий портал. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit_2019/zvit-npu-2019.pdf (дата звернення: 12.10.2021).

8. Звіт Голови Національної поліції України С. Князєва про результати роботи відомства за 2018 рік / Офіційний сайт Національної академії внутрішніх справ. URL: https://www.naiau.kiev.ua/files/news/2018/Zvit_NPU_2018.pdf (дата звернення: 12.10.2021).

9. Статистична інформація про стан злочинності та результати прокурорсько-слідчої діяльності / Офіційний сайт Генеральної прокуратури України. URL: https://old.gp.gov.ua/ua/statinfo.html (дата звернення: 26.09. 2021).

10. Звіт Національної поліції України про результати роботи у 2020 році. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2020/npu-zvit-2020.pdf (дата звернення: 18.10.2021).

11. Гавловський В. Д. Аналіз стану кіберзлочинності в Україні. *Інформація і право*. 2019. № 1 (28). С. 108–117. URL: https://mndcentr.com/vydania/pdf_publ/gv_28_19.pdf. (дата звернення: 15.09.2021).

12. Гуцалюк М. В. Сучасні тенденції організованої кіберзлочинності. *Інформація і право.* 2019. № 1 (28). С. 118–128. URL: http://ippi.org.ua/sites/default/files/15_9.pdf (дата звернення: 26.09.2021).

13. Кіберполіція попереджає про активізацію хакерів в період карантину / Офіційний сайт кіберполіції України. URL: https://cyberpolice.gov.ua/news/kiberpolicziya-poperedzhaye-pro-aktyvizacziyu-xakeriv-v-period-karantynu-617/ (дата звернення: 06.10. 2021).

14. Шепітько В. Ю. Інновації в криміналістиці як віддзеркалення розвитку науки. *Інноваційні методи та цифрові технології в криміналістиці, судовій експертизі та юридичній практиці* : матеріали міжнар. «круглого столу» (Харків, 12 груд. 2019 р.) / редкол. : В. Ю. Шепітько (голов. ред.), В. А. Журавель, В. М. Шевчук, Г. К. Авдєєва. Харків : Право, 2019. С. 147–150.

15. Що таке комп'ютерна криміналістика (форензіка)? *GROSS digital forensics Lab.* 2017. URL: https://g-ross.com.ua/novyny/kompyuterna-kryminalistyka-forenzika.html (дата звернення: 06.10.2021).

16. Домашенко О. М. Проблемні питання використання цифрових доказів у криміналістиці. *Інноваційні методи та цифрові технології в криміналістиці, судовій*

експертизі та юридичній практиці : матеріали міжнар. «круглого столу» (Харків, 12 груд. 2019 р.) / редкол.: В. Ю. Шепітько (голов. ред.), В. А. Журавель, В. М. Шевчук, Г. К. Авдєєва. Харків : Право, 2019. С. 52–55.

17. Що таке цифрова криміналістика*? GROSS digital forensics Lab.* 2018. URL: https://g-ross.com.ua/novyny/cyfrova-kryminalistyka-2.html (дата звернення: 29.09.2021).

18. Прокопенко С. Практика та особливості проведення комп'ютерно-технічних експертиз. *Матеріали IV Всеукраїнської конференції з кримінального права та процесу*. Київ, 2017. URL: https://www.slideshare.net/cyberlab_ua/ss-81935770 (дата звернення: 29.09.2021).

19. Popular Computer Forensics Top 21 Tools [Updated for 2019]. *Infosec*. 2019. URL: https://resources.infosecinstitute.com/computer-forensics-tools/#gref (дата звернення: 06.10.2021).

20. Android research and analysis tool Andr Ex R. *AOS company*. URL: https://www.fss.jp/android_andrex_r/ (дата звернення: 26.09.2021).

21. AOS Image Analysis Forensics Professional. *AOS company*. URL: https://www.fss.jp/fss_movie01-2/ (дата звернення: 26.09.2021).

22. フォレンジック製品 | DemiUAv3. *AOS company*. URL: https://www.fss.jp/%E3%83%95%E3%82%A9%E3%83%AC%E3%83%B3%E3%82%B8%E3%83%83%E3%82%AF%E8%A3%BD%E5%93%81%EF%BD%9Cdemiuav3/ (дата звернення: 29.09.2021).

23. DeceptionGrid – A Powerful Defense for Advanced Threats. *TrapX Security.* 2019. URL: https://trapx.com/wp-content/uploads/2019/05/PB-DeceptionGridv6.3-1-1.pdf (дата звернення: 24.09.2021).

24. TrapX Security DeceptionGrid 6.3. *SC Media magazine*. 14 August 2019. URL: https://www.scmagazine.com/review/trapx-security-deceptiongrid-6-3/ (дата звернення: 24.09.2021).

Павлюк Н. В., канд. юрид. наук, доцент кафедры криминалистики, Национальный юридический университет имени Ярослава Мудрого, Украина, г. Харьков.

e-mail: nat.pavluk.np@gmail.com ; ORCID 0000-0001-8058-3071.

Интеграция инновационных технологий в деятельности по расследованию преступлений – ведущее направление повышения ее эффективности

Статья посвящена одному из современных и приоритетных направлений научно-технического обеспечения следственной деятельности. Подчеркнуто, что борьба с киберпреступностью является одним из важнейших вопросов современности. Сделан вывод, что в условиях распространения в современном мире киберпреступности, одним из приоритетных направлений научно-технического обеспечения следственной деятельности является внедрение новейших средств, методов и технологий электронного интеллекта для работы с электронными доказательствами и защиты источников электронной (цифровой) информации.

Ключевые слова: электронный интеллект; информационно-коммуникационные технологии; научно-техническое обеспечение; следственная деятельность; цифровая криминалистика.

Pavliuk N. V., PhD in Law, Associate Professor of Department of Criminalistics, Yaroslav Mudryi National Law University, Ukraine, Kharkiv.

e-mail: nat.pavluk.np@gmail.com ; ORCID 0000-0001-8058-3071

Integration of innovative technologies into crime investigation activity is the significant direction of its effectiveness increasing

The article is devoted to the issues of the scientific and technical support of investigative activity. It is emphasized that nowadays fighting cybercrime determines the necessity to develop and implement the scientific and technical means, techniques and methods, as well as apply them to the

activity of law enforcement agencies for prevention and investigation of crimes in the field of information and telecommunication technologies.

The focus is placed on the fact that the retrieval, recording and investigation of electronic (digital) information in the pretrial investigation and its further use as evidence remain among the pressing and, at the same time, unexplored issues. It was stated that digital forensics is an integral and necessary tool in fighting cybercrime which is used for the identification, preservation, recovery, analysis, and presentation of digital evidence.

The conclusion was made that with the spread of cybercrime in the modern world one of the priority directions of scientific and technical support of investigative activity is introduction of the latest means, methods and technologies of electronic intelligence into the work with electronic evidence and also protection of the sources of electronic (digital) information.

Keywords: fighting cybercrime; electronic intelligence; electronic information; information and communication technologies; scientific and technical support; investigative activity; digital forensics.

References

1. Shepitko, V.Yu., Zhuravel, V.A., Avdieieva. H.K. et al. (2017). Informatsiini zasady tekhniko-kryminalistychnoho zabezpechennia diialnosti orhaniv kryminalnoi yustytsii. Kharkiv: Apostil [in Ukrainian].

2. Bernaz, P.V. (2015). Innovatsii – osnova kryminalistychnoho zabezpechennia diialnosti z rozsliduvannia zlochyniv. *Pivdennoukrainskyi pravnychyi chasopys, 4, 49–53* [in Ukrainian].

3. Kobets, M.V. (2006). Naukovo-tekhnichne zabezpechennia rozkryttia ta rozsliduvannia zlochyniv, poviazanykh z vybukhamy. *Extended abstract of candidate's thesis*. Kyiv: Kyiv. nats. un-t vnutr. sprav [in Ukrainian].

4. Palamarchuk, S.S. (2004). Naukovo-tekhnichne zabezpechennia poshuku slidiv zlochynu u vodnomu seredovyshchi. *Naukovyi visnyk Nats. akad. vnutr. sprav Ukrainy, 2, 110–122* [in Ukrainian].

5. Udalova, L.D. (2009). Naukovo-tekhnichne zabezpechennia otrymannia verbalnoi informatsii. *Zasady kryminalnoho sudochynstva ta yikh realizatsiia v zakonotvorchii i pravozastosovnii diialnosti : tezy dop. ta povidoml. nauk.-prakt. konf.* (Kyiv, 3 kvit. 2009 r.). Kyiv: Atika, *435–440* [in Ukrainian].

6. Bilenchuk, P., Malii, M. (2019). Kosmichna y elektronna kiberzlochynnist: zahrozy i vyklyky novoho tysiacholittia. *Lexinform. Yurydychni novyny Ukrainy*. URL: https://lexinform.com.ua/dumka-eksperta/kosmichna-j-elektronna-kiberzlochynnist-zagrozy-i-vyklyky-novogo-tysyacholittya/ [in Ukrainian].

7. Zvit Holovy Natsionalnoi politsii Ukrainy pro rezultaty roboty vidomstva u 2019 rotsi. (2019). *Uriadovyi portal.* URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit_2019/zvit-npu-2019.pdf [in Ukrainian].

8. Zvit Holovy Natsionalnoi politsii Ukrainy S. Kniazieva pro rezultaty roboty vidomstva za 2018 rik. *Ofitsiinyi sait Natsionalnoi akademii vnutrishnikh sprav*. (2018). URL: https://www.naiau.kiev.ua/files/news/2018/Zvit_NPU_2018.pdf [in Ukrainian].

9. Statystychna informatsiia pro stan zlochynnosti ta rezultaty prokurorsko-slidchoi diialnosti. *Ofitsiinyi sait Heneralnoi prokuratury Ukrainy.* (2020). URL: https://old.gp.gov.ua/ua/statinfo.html [in Ukrainian].

10. Zvit Natsionalnoi politsii Ukrainy pro rezultaty roboty u 2020 rotsi. (2020). URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2020/npu-zvit-2020.pdf [in Ukrainian].

11. Havlovskyi,V.D. (2019). Analiz stanu kiberzlochynnosti v Ukraini. *Informatsiia i pravo–Information and law, 1 (28), 108–117*. URL: https://mndcentr.com/vydania/pdf_publ/gv_28_19.pdf. [in Ukrainian].

12. Hutsaliuk, M.V. (2019). Suchasni tendentsii orhanizovanoi kiberzlochynnosti.

Informatsiia i pravo–Information and law, 1 (28), 118–128. URL: http://ippi.org.ua/sites/default/files/15_9.pdf [in Ukrainian].

13. Kiberpolitsiia poperedzhaie pro aktyvizatsiiu khakeriv v period karantynu. *Ofitsiinyi sait kiberpolitsii Ukrainy*. (2020). URL: https://cyberpolice.gov.ua/news/kiberpolicziya-poperedzhaye-pro-aktyvizacziyu-xakeriv-v-period-karantynu-617/ [in Ukrainian].

14. Shepitko, V.Yu. (2019) Innovatsii v kryminalistytsi yak viddzerkalennia rozvytku nauky. *Innovatsiini metody ta tsyfrovi tekhnolohii v kryminalistytsi, sudovii ekspertyzi ta yurydychnii praktytsi : materialy mizhnar. «kruhloho stolu»* (Kharkiv, 12 hrud. 2019 r.). Kharkiv: Pravo, *147–150* [in Ukrainian].

15. Shcho take kompiuterna kryminalistyka (forenzika)? (2017). *GROSS digital forensics Lab*. URL: https://g-ross.com.ua/novyny/kompyuterna-kryminalistyka-forenzika.html [in Ukrainian].

16. Domashenko, O.M. (2019) Problemni pytannia vykorystannia tsyfrovykh dokaziv u kryminalistytsi. *Innovatsiini metody ta tsyfrovi tekhnolohii v kryminalistytsi, sudovii ekspertyzi ta yurydychnii praktytsi : materialy mizhnar. «kruhloho stolu»* (Kharkiv, 12 hrud. 2019 r.). Kharkiv: Pravo, *52–55* [in Ukrainian].

17. Shcho take tsyfrova kryminalistyka? (2018). *GROSS digital forensics Lab*. URL: https://g-ross.com.ua/novyny/cyfrova-kryminalistyka-2.html [in Ukrainian].

18. Prokopenko, S. (2017). Praktyka ta osoblyvosti provedennia kompiuterno-tekhnichnykh ekspertyz. *Materialy IV Vseukrainskoi konferentsii z kryminalnoho prava ta protsesu*. Kyiv. URL: https://www.slideshare.net/cyberlab_ua/ss-81935770 [in Ukrainian].

19. Popular Computer Forensics Top 21 Tools [Updated for 2019]. (2019). *Infosec.* URL: https://resources.infosecinstitute.com/computer-forensics-tools/#gref.

20. Android research and analysis tool Andr Ex R. *AOS company.* URL: https://www.fss.jp/android_andrex_r/ [in Japan].

21. AOS Image Analysis Forensics Professional. *AOS company.* URL: https://www.fss.jp/fss_movie01-2/ [in Japan].

22. フォレンジック製品 | DemiUAv3. *AOS company.* URL: https://www.fss.jp/%E3%83%95%E3%82%A9%E3%83%AC%E3%83%B3%E3%82%B8%E3%83%83%E3%82%AF%E8%A3%BD%E5%93%81%EF%BD%9Cdemiuav3/ [in Japan].

23. DeceptionGrid – A Powerful Defense for Advanced Threats. (2019). *TrapX Security.* URL: https://trapx.com/wp-content/uploads/2019/05/PB-DeceptionGridv6.3-1-1.pdf.

24. TrapX Security DeceptionGrid 6.3. (2019). *SC Media magazine, 14 August*. URL: https://www.scmagazine.com/review/trapx-security-deceptiongrid-6-3/.

Надійшла до редколегії 19.10.2021 р.